ISSN: 2338-8412 e-ISSN : 2716-4411

Ekombis Review – Jurnal Ilmiah Ekonomi dan Bisnis
Available online at : https://jurnal.unived.ac.id/index.php/er/index
DOI: https://doi.org/10.37676/ekombis.v13i4

Literature Review Of The Role Of Strategic Management Accounting Through Mitigation Measures Against Ransomware Attacks

Yuni Astuti [1], Daniel Nugroho [2], Yanuar Ramadhan [3]
[1,2,3] Universitas Esa Unggul
Email: [1] astutiyuni0606@student.esaunggul.ac.id , [2] nugroho.daniel86@student.esaunggul.ac.id
[3] yanuar.ramadhan@esaunggul.ac.id

How to Cite :
Astuti, Y., Nugroho, D., Ramadhan, Y. (2025). Literature Review Of The Role Of Strategic management Accounting Through Mitigation Measures Against Ransomware Attacks. EKOMBIS REVIEW: Jurnal Ilmiah Ekonomi Dan Bisnis, 13(4). DOI: https://doi.org/10.37676/ekombis.v13i4

ARTICLE HISTORY
Received [14 May 2025]
Revised [24 September 2025]
Accepted [29 September 2025]

KEYWORDS
Strategic Management Accounting, Cybersecurity, Ransomware, Risk Mitigation, Governance.

ABSTRACT

The massive wave of digital transformation has increased organizational exposure to cybersecurity threats, particularly ransomware, which poses significant financial impacts. Ransomware is no longer merely a technical issue but a strategic challenge requiring a multidisciplinary mitigation approach. This study aims to examine the role of strategic management accounting in supporting mitigation efforts against ransomware attacks through a systematic literature review (SLR). The method applied is an SLR of 20 Sinta-indexed journals (levels 1–4) published between 2020 and 2024. The study was conducted from January to March 2025. The analysis reveals that strategic management accounting contributes through the integration of monitoring technologies, the development of risk governance frameworks, strengthening of organizational security culture, and optimization of security systems. Strategic management accounting also supports data-driven decision-making regarding resource allocation and security investment evaluation. This study suggests the need for synergy between accounting and information technology professionals to enhance organizational resilience. The findings offer both theoretical and practical contributions for developing more integrated and adaptive cybersecurity strategies in the face of evolving ransomware threats.

INTRODUCTION

Attack *ransomware* has develop from threat technical become challenge strategic multidimensional which requires approach management comprehensive . “Global losses from *ransomware attacks are estimated* to reach 20 billion USD in 2021, a 57-fold increase compared to 2015” (Mulianingsih, 2025). Global statistics show a worrying trend related attack *ransomware* . According to report *International Business Machines* (IBM), “ the average cost of a global data

breach has reached 4.45 million US dollar , with attack *ransomware* donate portion significant from loss " . (Shakib et al., 2025)In Indonesia itself , the National Cyber and Crypto Agency (BSSN) noted happen more of 1,400 attacks cyber every day throughout in 2022, with 30% of them in the form of attack *ransomware* that targets institution finance and business scale big . " In the last five years, *ransomware* attacks worldwide including in Indonesia have shown a fairly high spike. According to a report from *Bitdefender , ransomware* attacks increased by 485% from 2019 to 2020, and this trend continues with increasing complexity of attacks (Alzakari et al., 2025). "

In Indonesia, ransomware attacks occurred in several sectors, one of which occurred in the health sector," the Siloam Hospital information system in 2021, where patient data was encrypted and attackers demanded a ransom in the form of *cryptocurrency ,* this shows that the health sector is very vulnerable to cyber attacks " (Wijanarko et al., 2023). In addition, towards the end of 2021, Bank Indonesia confirmed the Conti ransomware attack that occurred at the Bengkulu branch office. Although no critical data was leaked, some data was successfully uploaded to the dark web (Cyberthreat, 2022). In addition, in May 2023, Bnak Syariah Indonesia (BSI) experienced a disruption that was initially claimed as system maintenance, however, after a few days, it was revealed that they were attacked by LockBit, which demanded a ransom of IDR 200 billion and threatened to leak customer data (Hardeva, 2023). Data from *Cybersecurity* Indonesia also shows that *ransomware attacks* in the government sector are increasing, with more than 50% of government agencies experiencing cyber attacks in the form of ransomware in the last three years . Attacks on government information systems can result in the loss of important data and disruption of public services. Fundamentally *ransomware* is threat security technology impactful information financial for management strategic ." Involvement accountancy management strategic in context mitigation covers evaluation investment security ,analysis cost-benefit from implementation technology security , development indicator performance related security, as well as planning and budgeting for security program cyber " (Nurwanah, 2024).

In literature academic contemporary , has start formed awareness will importance integration between management security cyber with system accountancy management . According to (Temitayo Oluwaseun Abrahams et al., 2023), " framework Work accountancy management strategic can applied For measure and evaluate investment security cyber ". In line with matter This According to (Kalinaki, 2025)" approach accountancy management based on risk can in a way significant increase effectiveness of security programs cyber organization through allocation source more optimal power. Although study previous has confess relevance accountancy management in context security cyber , there is gap significant in literature about How practice accountancy management strategic in a way specific that can contribute to mitigation risk ransomware attacks.

Based on the description above , can concluded that there is need urge For explore in a way more deep about role accountancy management strategic in mitigation risk ransomware attack . Exploration This No only relevant from perspective academic For fill in gap in literature , but also has implications significant practical for organization that seeks increase resilience to threat increasingly cyber complex ., research This aiming For do review literature comprehensive about role accountancy management strategic in develop and implement steps mitigation to ransomware attacks , with focus specifically in the Indonesian context. Formulation problem in study This is : (1) How framework accountancy management strategic can applied For identify , measure , and manage risk ransomware attacks ? (2) What are they? approaches and tools analysis in accountancy management strategic that can support mitigation strategy development effective ransomware attack ? (3) How practice best in integrate perspective accountancy management to in security program cyber organization, especially in context mitigation ransomware risk?. Study this is also expected can give implications significant managerial with highlight How professional accountancy management

can collaborate with professional security cyber For develop effective and efficient mitigation strategies. By Thus , the study This No only relevant for academics in field accountancy management and security cybe, but also for practitioners and makers policy of interest in increase resilience organization to threat cyber contemporary.

LITERATURE REVIEW

Ransomware

Ransomware is a type of malware that encrypts user data and demands a ransom to decrypt it. According to the Cybersecurity & Infrastructure Security Agency (CISA, 2021), “ransomware attacks have increased significantly in recent years, with more than 4,000 attacks occurring every day. The types of ransomware vary, from ransomware that encrypts personal files to ransomware that attacks the operating system” Overall. Ransomware can be divided into several types based on how it works. “Encrypting ransomware, which encrypts files and demands a ransom for the decryption key such as CryptoLocker, which first appeared in 2013 and infected thousands of computers by demanding a ransom in Bitcoin” (Ariyanto, 2024). In addition, there is also locker ransomware that does not encrypt files, but locks access to the operating system or device. An example of this type is Police ransomware. “Police ransomware displays a fake message from the authorities and demands a ransom to unlock the device” (Shakib et al., 2025). According to (Wany et al., 2024) "locker ransomware is often easier to overcome than encrypting ransomware, but can still cause significant disruption to users". Ransomware can also be categorized based on its distribution method, such as phishing, "exploit kits, and remote desktop protocol (RDP). Phishing, which involves sending malicious emails more than 90% of cyber attacks start with phishing to steal user information" (G. Ramadhan, 2023)

Strategic Management Accounting

Strategic management accounting is a process that integrates accounting information with corporate strategy to support better decision making. According to Simon (1981), "management accounting is the provision and analysis of data about a business and its competitors for use in developing and monitoring business strategies" strategic management accounting not only focuses on financial statements, but also includes cost analysis, planning, and operational control that are oriented towards achieving the company's long-term goals. "Companies that implement strategic management accounting effectively can increase profitability by up to 25% compared to companies that do not" (Masitoh & Santoso, 2022). In the research conducted by (Bonnici & Galea, 2015) companies that integrate Strengths, Weaknesses, Opportunities, Threats (SWOT) analysis with accounting information can identify better market opportunities and reduce the risks associated with strategic decisions.

METHODS

This study uses the Systematic Literature Review (SLR) method, which is a secondary research approach to identify, evaluate, and interpret all available literature related to a particular research topic. The SLR approach was chosen because of its ability to provide a comprehensive understanding of the development of studies on the role of strategic management accounting in mitigating ransomware cybersecurity attacks, as well as identifying research gaps that can be directions for further research.

The SLR method allows for systematic mapping of conceptual and empirical developments related to the topic being studied, taking into account the reliability and validity aspects of the knowledge synthesis process carried out. The implementation of this research began in March 2025 and was completed in May 2025, focusing on scientific publications published between 2020 and 2024. The SLR research procedure in this study adopts the framework developed by

Kitchenham and Charters with modifications adapted to the context of management accounting and cybersecurity. The stages carried out include review planning, review implementation, and reporting of review results. At the planning stage, research needs are identified and review protocol development is carried out which includes research questions, search strategies, inclusion and exclusion criteria, and data extraction and synthesis strategies. This review protocol was developed by referring to previous studies conducted in the context of strategic management accounting research.

The data sources in this study were scientific articles indexed in the Science and Technology Index (Sinta) and Scopus databases, which are scientific journal ranking and indexing systems. The search was conducted on journals with Scopus and Sinta categories with a focus on the fields of accounting, management, information systems, and information security. This study used a combination of Indonesian and English keywords, including: "strategic management accounting", "ransomware", "cyber security", "cyber risk mitigation", "strategic management accounting", "cyber security", "cyber risk mitigation", and "ransomware attack".

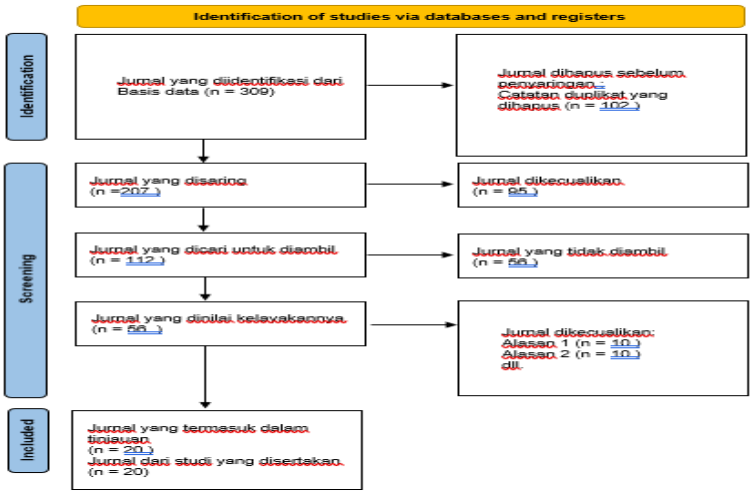
The data collection technique was carried out through several systematic stages. The first stage was an initial search using keywords that had been set on the Sinta portal and related journal databases. This search resulted in 78 potential articles which then went through a screening stage based on inclusion and exclusion criteria. Inclusion criteria include: (1) articles published in journals indexed by Scopus and Sinta 1&2 (2) articles published between 2020-2024, (3) articles discussing management accounting, cybersecurity, or both, and (4) articles available in full text. Meanwhile, exclusion criteria include: (1) articles focusing on technical aspects of cybersecurity without any relation to management or accounting, (2) articles in the form of editorials, book reviews, or short communications, and (3) duplicate articles. The screening process produced 43 articles which were then tested for eligibility through a quality assessment using an instrument adapted from Wasono and Furinto (2022). In the end, 20 articles were obtained that met the quality threshold for further analysis. The data analysis technique in this study applies a qualitative meta-synthesis approach with a meta-aggregation technique as recommended by the Joanna Briggs Institute.

This technique allows researchers to integrate findings from various qualitative studies without transforming the original data, thus maintaining the integrity of the initial findings. The analysis process is carried out in stages: (1) data extraction from selected articles using a validated extraction form, (2) categorization of findings based on emerging themes and subthemes, (3) aggregation of findings to produce a comprehensive synthesis, and (4) assessment of the level of confidence in the aggregate findings using the ConQual framework.

The validity and reliability of the study are maintained through several strategies. First, researchers use a clear and detailed review protocol to ensure consistency in the article selection and analysis process. Second, the data selection and extraction process is carried out independently by two researchers, with a consensus meeting to address differences in assessment. Third, preliminary findings are validated through discussions with management accounting and cybersecurity experts. Fourth, triangulation of data sources is carried out by comparing articles from various types of journals and research perspectives. This approach is in line with recommendations to ensure the quality of SLR research in the field of management accounting.

RESULTS

Figure 1. PRISMA Flowchart



Systematic review literature conducted against 20 journals indexed Sinta has produce a number of findings important about role accountancy management strategic in mitigation cyber security ransomware attacks . Analysis to articles selected produce synthesis that can grouped to in four category main : (1) integration technology in accountancy management strategic For security cyber , (2) governance and management framework risk , (3) factors organizational in implementation security cyber , and (4) innovation and optimization system security . Distribution article based on category This served in Table 1.

Table 1. Distribution of Articles Based on Category Findings

No	Category Findings	Number of Articles	Percentage (%)
1	Technology Integration in Accountancy Management Strategic	7	35
2	Governance and Management Framework Risk	5	25
3	Organizational Factors in Implementation Cyber Security	4	20
4	Innovation and Optimization System Security	4	20

Apart from categorization based on theme findings , analysis was also carried out to approach methodology used in articles mentioned . As shown in Table 2, there are variation method significant research , with domination approach quantitative and implementation system , which reflects balance between exploration conceptual and application practical in study related accountancy management strategic and security cyber.

Table 2. Distribution of Articles Based on Methodology Study

No	Methodology Study	Number of Articles	Percentage (%)
1	Quantitative	6	30
2	Implementation System	6	30
3	Case study	3	15
4	Literature Review	3	15
5	Qualitative	2	10

Based on analysis to journals said , it was found existence evolution significant in contribution accountancy management strategic to mitigation cyber security attacks , in particular *ransomware.* Publication trends show improvement amount study related Topic This in five years Lastly , with concentration highest in 2024-2025 , indicating relevance and urgency issue This in context science contemporary.

DISCUSSION

Technology Integration in Strategic Management Accounting for Cybersecurity

Findings from the literature analysis indicate that technology integration in strategic management accounting practices has a significant role in increasing the effectiveness of mitigating cybersecurity attacks, especially ransomware. Irmanto et al. (2024) in their study on personnel position monitoring systems using GPS emphasized the importance of real-time human resource monitoring with a success rate of 98.6%. This type of system contributes to strategic management accounting by optimizing human resource allocation and increasing rapid response to security threats, which can be applied in the context of cyber attacks. This finding is in line with the results of the study (Aripilahi et al., 2024). who implemented Wazuh for network security monitoring and successfully detected unauthorized file modifications early, a capability that is very crucial in preventing ransomware attacks. The application of artificial intelligence and machine learning technologies has also emerged as a significant trend in technology integration with strategic management accounting. (Hairani & Widiyaningtyas, 2024) demonstrated how Convolutional Neural Networks (CNN) with data augmentation can achieve very high detection accuracy (99.7%).

Although this study focused on rice plant disease detection, similar methodologies can be transferred to the context of cybersecurity to detect anomalies that indicate potential ransomware attacks. Furthermore, Muhammadiyah (2025) confirmed the effectiveness of combining classical data augmentation techniques with Deep Convolutional Generative Adversarial Networks (DCGAN) which achieved an accuracy of 98.13%. The application of such data augmentation techniques can significantly improve the capabilities of cyberattack detection models, providing an additional layer of protection against ransomware. In terms of data management, research on satellite telemetry data information systems (not mentioned by the author) highlights the importance of big data management systems for strategic analysis and decision making. The system, which was successfully developed with a success rate of 86.22%, shows how the System Development Life Cycle (SDLC) approach can produce an integrated data security system that prevents unauthorized access, a fundamental principle in mitigating ransomware attacks. This finding is reinforced by a study (Junaidi et al., 2022) which implemented a computer network monitoring system using Icinga, enabling early anomaly detection with efficient use of computing resources (less than 20%). This kind of efficiency is an important consideration in strategic management accounting which emphasizes resource optimization.

Governance and Risk Management Framework

Aspects of governance and risk management emerge as essential components in the integration of strategic management accounting with cybersecurity attack mitigation strategies. (Darmi et al., 2024) through an evaluation of information system security governance based on Control Objectives for Information and Related Technologies (COBIT) 2019 identified a gap of 2 levels from what was expected in the APO12 (risk management) and BAI10 (configuration management) domains. This finding highlights the urgency of developing information system governance performance metrics that are integrated with management accounting for strategic decision making that can minimize security gaps. In line with that, Kosadi et al. (2020) in their literature study on corporate governance in Indonesia underlines how good governance can

prevent financial fraud, including those originating from cyber attacks. This study, although more oriented towards general aspects of corporate governance, provides a foundation for understanding the relationship between governance practices and financial information security risk mitigation.

This finding is confirmed by research (Isnaini & Suhartono, 2023) which analyzed the security of village administration applications using the Mobile Security Framework and ISO 27002:2013, revealing vulnerabilities in the cryptography and access permissions aspects. This study highlights the importance of standardizing business processes and information risk management—key elements in strategic management accounting—as a foundation for implementing effective access control and cryptography in protecting sensitive data from cyber attacks. In a broader perspective, research (Natalia Baba, 2024) on the relationship between ethical leadership, accountability, and technological transformation highlights the vital role of ethical leadership that emphasizes moral values in enhancing technological innovation. This literature review of 82 multidisciplinary articles underlines the importance of ethics in strategic decision-making, including in the context of implementing cybersecurity and handling data breaches. This ethical aspect complements the technical and managerial dimensions in a comprehensive governance framework for mitigating cybersecurity risks.

Organizational Factors in Cybersecurity Implementation

The organizational dimension plays a crucial role in the context of implementing a cybersecurity mitigation strategy. (Fridayani & Kusuma, 2024) examined the effect of organizational agility on social sustainability and found that organizational agility significantly influenced organizational support, organizational culture, and social sustainability. This study highlights how organizational security culture can strengthen resilience to cyberattacks—an aspect that is often overlooked in technical approaches to information security. Furthermore, Habib et al. (2025) through Structural Equation Modeling analysis confirmed that perceived security greatly influences user trust (0.651) in digital services, which in turn impacts perceived usefulness (0.576) and satisfaction (0.527).

These findings emphasize the importance of the perceptual dimension in implementing security technology, which must be considered in a comprehensive management accounting strategy. In line with that, (R. Ramadhan et al., 2025) identified that human and organizational factors significantly influence the adoption of cloud-based accounting in the Indonesian banking sector. This study highlights the importance of considering non-technical factors in the adoption of modern accounting technology that have implications for data security in accounting systems. Other organizational aspects that need to be considered are business strategy and innovation. (Cuandra & Candy, 2024) in their research on strategy and innovation to improve the sustainable performance of SMEs in the digital business era found a significant impact of technological, learning, and relational capabilities on SME performance. This study emphasizes that technological capabilities are an important factor in the security of SME information systems, which must be integrated into business strategies for sustainable performance.

Innovation and Optimization of Security Systems

Innovation in security systems is an aspect that is no less important in mitigating cyber security attacks. Priyanto and Azhar (2017), although a relatively older study, highlighted the effectiveness of the Data Encryption Standard (DES) algorithm for data encryption with a processing speed of 3 seconds per file capacity of 1024 bytes. This kind of data encryption approach is a fundamental defense against ransomware attacks that access sensitive data. Meanwhile, (Hariyadi & Juliansyah, 2018) demonstrated the implementation of private cloud computing based on Proxmox Virtual Environment that supports high availability with four servers.

This study highlights how virtualization and setting access with limited logins can improve data security as well as cost efficiency aspects that are very relevant to strategic management accounting principles. Optimization of security systems can also be improved through an optimization algorithm approach. (Ardina & Sari, 2025) applied the Artificial Bee Colony (ABC) method to optimize the location of electric vehicle charging stations and successfully identified the shortest distance from the initial location to the optimal location. Although not directly related to cybersecurity, this kind of optimization methodology can be adapted to optimize the configuration of cybersecurity systems. Similarly, (Silva & Braeken, 2025) analyzed the reliability of acoustic features in various environments and found that Mel-frequency Cepstral Coefficients (MFCCs) showed excellent reliability with high correlation coefficients (0.98819 and 0.98889). This kind of acoustic fingerprinting technique opens up innovative opportunities for development in security systems that can detect operational anomalies that indicate cyber attacks. Another aspect of innovation is seen in the study (Hidayatullah et al., 2025) which analyzed Twitter conversations related to the Indonesian presidential election using a clustering algorithm. The Agglomerative Hierarchical Clustering method with Ward linkage produced the highest Silhouette Score (0.8018), indicating its effectiveness in identifying communication patterns. This kind of methodology can be transferred into the context of cybersecurity to identify malicious communication patterns related to cyberattacks, including ransomware. Meanwhile, a study (Luhur et al., 2023) on the Estonian e-Residency program highlights the importance of digital identity security as a crucial component in mitigating cyberattacks in the context of global digital business models.

Synthesis and Implications for Strategic Management Accounting

Based on a comprehensive analysis of 20 selected journals, it can be synthesized that the role of strategic management accounting in mitigating ransomware cybersecurity attacks includes several main dimensions. First, integrating advanced technologies such as artificial intelligence, machine learning, and real-time monitoring systems into the management accounting decision-making framework can significantly improve the capabilities of early detection and response to ransomware threats. Second, developing a governance and risk management framework integrated with management accounting principles enables more optimal resource allocation for cybersecurity initiatives. Third, organizational dimensions such as security culture, user trust, and organizational agility are critical factors that must be incorporated into a comprehensive cybersecurity management accounting strategy. Fourth, continuous innovation in security systems, supported by a value-oriented management accounting approach, can improve organizational resilience to increasingly sophisticated ransomware attacks.

The implications of these findings for strategic management accounting practices are substantial. Management accounting professionals need to develop a deeper understanding of cybersecurity technologies and work more closely with information technology professionals to integrate security considerations into strategic decision-making processes. The development of performance metrics that incorporate cybersecurity dimensions is also becoming increasingly important to support a more comprehensive evaluation of security investments. Furthermore, integrating organizational factors into a cybersecurity management accounting framework can improve the effectiveness of overall ransomware mitigation strategy implementation.

CONCLUSION

Based on the results of a systematic literature review of 20 research journals, it is concluded that strategic management accounting plays an important role in mitigating ransomware attacks through the integration of information technology, governance and risk management frameworks, organizational dimensions, and security system innovations. Strategic

management accounting is able to provide a data-based and value-based approach in strategic decision-making related to cybersecurity, including resource allocation, security investment evaluation, and development of performance indicators related to cyber risk. These results indicate that a holistically integrated management accounting approach with a cybersecurity strategy can increase organizational resilience to increasingly complex and financially detrimental ransomware threats.

SUGGESTIONS

The suggestions that can be put forward from this study are the importance of increasing collaboration between management accounting and information technology professionals to develop a more adaptive cyber risk mitigation framework. First, organizations are advised to adopt analytical technology and artificial intelligence in management accounting systems to improve early detection of ransomware attacks. Second, the development of a security culture and ethical leadership needs to be integrated into organizational strategies to strengthen awareness and response to cyber threats.

Third, it is necessary to formulate policies that support the integration between strategic management accounting and compliance with cybersecurity regulations. Further research can examine the application of this framework in case studies of specific industrial sectors to produce more applicable practical guidelines.

REFERENCES

Agustin, T. (2025). *Optimizing Rice Plant Disease Classification Using Data Augmentation with GANs on Convolutional Neural Networks*. *9*(1), 97–114.

Hardeva, H. (2023). *Analisis Respon Komunikasi Krisis Bank Syariah Indonesia di Kompas.com Terkait Serangan Ransomware*.

Alzakari, S. A., Aljebreen, M., Ahmad, N., Alhashmi, A. A., Alahmari, S., Alrusaini, O., Al-Sharafi, A. M., & Almukadi, W. S. (2025). An intelligent ransomware based cyberthreat detection model using multi head attention-based recurrent neural networks with optimization algorithm in IoT environment. *Scientific Reports*, *15*(1). https://doi.org/10.1038/s41598-025-92711-4

Ardina, A. A., & Sari, R. K. (2025). *Artificial Bee Colony-Based Optimization for Public Electric Vehicle Charging Station Placement*. *9*(1), 115–127.

Aripilahi, E., Khairil, K., & Akbar, A. Al. (2024). Application Of Wazuh To Conduct Monitoring Network Security System (Case Study Of SMK N 1 Bengkulu City). *Jurnal Media Computer Science*, *3*(2), 125–136. https://doi.org/10.37676/jmcs.v3i2.6592

Ariyanto, S. (2024). Analisis Framing Model Robert N. Entman tentang Serangan Ransomware Pada PT Bank Syariah Indonesia Tbk. *Jurnal CommLine*, *9*(1), 59–77.

Bahmanova, A., & Lace, N. (2024). Cyber Risks: Systematic Literature Analysis. *Proceedings IMCIC - International Multi-Conference on Complexity, Informatics and Cybernetics*, *2024-March*(2), 177–184. https://doi.org/10.54808/IMCIC2024.01.177

Branham, M. B., & Branham, M. B. (2024). *Strategies Cybersecurity Professionals Use to Mitigate Cybersecurity Threats in Small Businesses Walden University This is to certify that the doctoral study by*.

Cuandra, F., & Candy, C. (2024). Strategies and Innovations for Enhancing Sustainable Performance in SMEs During The 4.0 Digital Business Era. *Jurnal Organisasi Dan Manajemen*, *20*(1), 1–16. https://doi.org/10.33830/jom.v20i1.6449.2024

Darmi, Y., Fernandez, S., Fathoni, M. Y., & Wijayanto, S. (2024). Evaluation of Governance in Information Systems Security to Minimize Information Technology Risks. *INTENSIF: Jurnal Ilmiah Penelitian Dan Penerapan Teknologi Sistem Informasi*, *8*(1), 40–51. https://doi.org/10.29407/intensif.v8i1.21221

Diptiben Ghelani. (2022). Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. *American Journal of Science, Engineering and Technology*, *3*(6), 12–19. https://doi.org/10.11648/j.XXXX.2022XXXX.XX

Fridayani, J. A., & Kusuma, S. E. (2024). The Role of Organizational Agility, Perceived Support, and Culture in Shaping Social Sustainability. *Jurnal Organisasi Dan Manajemen*, *20*(1), 65–84. https://doi.org/10.33830/jom.v20i1.7551.2024

Habib, A., Pramana, E., & Junaedi, H. (2025). *Extending the Expectation Confirmation Model to Examine Continuous Use Mobile Banking : Security , Trust , and Convenience*. *9*(1), 76–96.

Hairani, H., & Widiyaningtyas, T. (2024). Augmented Rice Plant Disease Detection with Convolutional Neural Networks. *INTENSIF: Jurnal Ilmiah Penelitian Dan Penerapan Teknologi Sistem Informasi*, *8*(1), 27–39. https://doi.org/10.29407/intensif.v8i1.21168

Halachev, P. (2024). A big data approach to risk management and control: Cybersecurity in accounting. *Periodicals of Engineering and Natural Sciences (PEN)*, *12*(2), 331. https://doi.org/10.21533/pen.v12i2.4021

Hariyadi, I. P., & Juliansyah, A. (2018). Analisa Penerapan Private Cloud Computing Berbasis Proxmox Virtual Environment Sebagai Media Pembelajaran Praktikum Manajemen Jaringan. *MATRIK : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, *18*(1), 1–12. https://doi.org/10.30812/matrik.v18i1.329

Herawan, A., Rachim, E., & Sutjipto, S. S. U. (2022). Design of LAPAN-A2 Satellite Telemetry Data Information System Using SDLC. *INTENSIF: Jurnal Ilmiah Penelitian Dan Penerapan Teknologi Sistem Informasi*, *6*(1), 43–55. https://doi.org/10.29407/intensif.v6i1.16149

Hidayatullah, S., Nuraini, U. S., & Surabaya, U. N. (2025). *Uncovering Key Topics in Indonesian Political Discourse Through Twitter Analysis After the 2024 Presidential Inauguration Using Clustering methods*. *9*(1), 128–146.

Irmanto, D., Sujito, S., Aripriharta, A., Widiatmoko, D., Kasiyanto, K., & Omar, S. (2024). Optimizing the Personnel Position Monitoring System Using the Global Positioning System in Hostage Release. *INTENSIF: Jurnal Ilmiah Penelitian Dan Penerapan Teknologi Sistem Informasi*, *8*(1), 91–107. https://doi.org/10.29407/intensif.v8i1.21665

Isnaini, K. N., & Suhartono, D. (2023). Security Analysis of Simpel Desa using Mobile Security Framework and ISO 27002:2013. *INTENSIF: Jurnal Ilmiah Penelitian Dan Penerapan Teknologi Sistem Informasi*, *7*(1), 84–105. https://doi.org/10.29407/intensif.v7i1.18742

Junaidi, I., Wahyudi, J., & Prasetiyo Rohmawan, E. (2022). Implementation of a Computer Network Monitoring System Using Icinga Linux-Based Ubuntu Server at SMA N 1 Bengkulu Tengah Penerapan Sistem Monitoring Jaringan Komputer Menggunakan Icinga Berbasis Linux Ubuntu Server Pada SMA N 1 Bengkulu Tengah. *Jurnal Komitek*, *2*(2), 629–636.

Kalinaki, K. (2025). Ransomware Threat Mitigation Strategies for Protecting Critical Infrastructure Assets. In *Ransomware Evolution* (pp. 120–143). CRC Press.

Kosadi, F., Jaya, R. C., & Hamdani, D. (2020). *Rentang kisah literatur tata kelola perusahaan Indonesia*. *9*(2021), 25–42.

Luhur, K. B., Trihartono, A., Hara, A. E., & Jember, U. (2023). *Navigating Digital Frontiers : Estonia ' s e-Residency through the Lens of the Eclectic Paradigm Menjelajahi Batas-Batas Digital : E-Residency Estonia melalui Sudut Pandang Paradigma Eklektik*. 121–142.

Masitoh, I., & Santoso, R. A. (2022). Analisis Kompetensi SDM Dan Independensi Audit Internal Terhadap Kualitas Laporan Audit. *Universitas Sangga Buana YPKP*, *1*(1).

Md Haris Uddin Sharif, & Mehmood Ali Mohammed. (2022). A literature review of financial losses statistics for cyber security and future trend. *World Journal of Advanced Research and Reviews*, *15*(1), 138–156. https://doi.org/10.30574/wjarr.2022.15.1.0573

Mulianingsih, F. (2025). *Manajemen Risiko Digital: Strategi Keamanan Siber untuk Mitigasi Ancaman di Era Revolusi Industri 4.0*. *5*, 888–898.

Natalia Baba, C. (2024). Ethical Leadership and Accountability: Technology Innovation. *Jurnal Konsep Bisnis Dan Manajemen)*, *10*(2), 2024. https://doi.org/10.31289/jkbm.v10i2.11489

Nurwanah, A. (2024). Cybersecurity in Accounting Information Systems: Challenges and Solutions. *Advances in Applied Accounting Research*, *2*(3), 157–168. https://doi.org/10.60079/aaar.v2i3.336

Wijanarko, R. P., Setiawan, R., Mukaromah, S., Rezha, A., & Najaf, E. (2023). *Prosiding Seminar Nasional Teknologi dan Sistem Informasi (SITASI) 2023 Surabaya*.

Perwej, Dr. Y., Qamar Abbas, S., Pratap Dixit, J., Akhtar, Dr. N., & Kumar Jaiswal, A. (2021). A Systematic Literature Review on the Cyber Security. *International Journal of Scientific Research and Management*, *9*(12), 669–710. https://doi.org/10.18535/ijsrm/v9i12.ec04

Priyanto, D., & Azhar, R. (2017). Sistem Aplikasi Untuk Keamanan Data Dengan Algoritma "Des" (Data Encryption Standard). *Jurnal Matrik*, *16*(1), 67. https://doi.org/10.30812/matrik.v16i1.12

Ramadhan, G. (2023). Perlidungan Hukum Bagi Korban Ransomware Wannacry Tindak Pidana Ransomware. *Jurnal Kajian Kontemporer Hukum Dan Masyarakat*, *1–25*, 1–2. DOI: 10.11111/dassollen.

Ramadhan, R., Farishi, A., & Tjun, L. T. (2025). *Factors Affecting Cloud-Based Accounting Adoption in the Indonesian Banking Sector*. *29*(01), 25–47.

Sammut-Bonnici, T., & Galea, D. (2015). Analysis Swot. In *Wiley Encyclopedia of Management* (pp. 1–8). Wiley. https://doi.org/10.1002/9781118785317.weom120103

Shakib, K. H., Rahman, M., Islam, M., & Chowdhury, M. (2025). Impersonation Attack Using Quantum Shor's Algorithm Against Blockchain-Based Vehicular Ad-Hoc Network. *IEEE Transactions on Intelligent Transportation Systems*. https://doi.org/10.1109/TITS.2025.3534656

Silva, B., & Braeken, A. (2025). *Environmental Acoustic Features Robustness Analysis : A Multi-Aspecs Study*. *9*(1), 46–59.

Temitayo Oluwaseun Abrahams, Sarah Kuzankah Ewuga, Simon Kaggwa, Prisca Ugomma Uwaoma, Azeez Olanipekun Hassan, & Samuel Onimisi Dawodu. (2023). Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security. *World Journal of Advanced Research and Reviews*, *20*(3), 1743–1756. https://doi.org/10.30574/wjarr.2023.20.3.2691

Vilakazi, K., & Adebesin, F. (2023). A Systematic Literature Review on Cybersecurity Threats to Healthcare Data and Mitigation Strategies. *EPiC Series in Computing*, *93*, 240–251. https://doi.org/10.29007/hf15

Wany, E., Widjaja1, A. T., & Budi Prayitno. (2024). Analisis Penggunaan Teknologi Informasi terhadap Efektivitas Audit Pajak. *Akuntansi : Jurnal Akuntansi Integratif*, *10*(1), 69–78. https://doi.org/10.29080/jai.v10i1.1574